социальные системы
www.socialsystems.ru

Программное обеспечение устройства работы с бесконтактными картами платёжной системы "МИР"

Эксплуатация программного обеспечения

Листов 18

Москва, 2023

Оглавление

Список сокращений

Сокращение	Расшифровка
AID	Application Identifier - номер платёжного приложения
CD-CVM	Consumer Device CVM – метод идентификации держателя карты с помощью устройства держателя
CDA	Combined Data Authentication – метод проверки легитимности EMV-карты, основанный как на динамических данных, так и статических
CRL	Certification Revocation List – список отозванных сертификатов
CVM	Cardholder Verification Method – метод идентификации владельца карты
DDA	Dynamic Data Authentication – метод проверки легитимности EMV-карты, основанный на динамических данных
EMV	Europay + MasterCard + VISA – международный стандарт для операций по банковским картам с чипами
SDA	Static Data Authentication – метод проверки легитимности EMV-карты, основанный на статических данных
TAC	Terminal Action Code
TVR	Terminal Verification Result
ПС	Платёжная система

Аннотация

Данный документ содержит описание функциональных характеристик программного обеспечения согласно спецификации бесконтактного платёжного ядра платёжной системы "МИР".

1. Общие сведения

Программное обеспечение устройства для работы с бесконтактными картами платёжной системы "МИР" (далее ядро "МИР") соответствует документу "Спецификация ядра бесконтактного ридера ПС 'МИР'", версии 2.3.0.

Для работы с ядром "МИР" необходимо предварительно скомпилировать, собрать его под определённую аппаратную платформу и установить. Процесс сборки и установки ПО лежит за рамками этого документа. Подразумевается, что аппаратная платформа, на которое производится установка, обладает необходимым функционалом реализации физического уровня протокола ISO/IEC 14443(A/B), другими словами, должна иметь в своём составе микросхему NFC. Для упрощения здесь и далее предлагается называть такую аппаратную платформу ридером или устройством.

Для управления ридером и обмена данными с ридером должен быть разработан протокол, реализующий набор необходимых команд для эксплуатации функций программных модулей, установленных на ридер, в частности одним из таких модулей должно быть ядро "МИР".

Для управления ридером по разработанному протоколу необходима реализация так называемой терминальной программы или терминального ПО, которое может быть установлено на другое устройство и осуществлять взаимодействие с ридером в автоматическом режиме, либо такое ПО может быть выполнено в виде программы как с графическим интерфейсом, так и без него, установленной на ПЭВМ и работающей по командам или манипуляциям человека-оператора.

В данном документе предлагается описание эксплуатации ядра МС по второму варианту, где в качестве терминального ПО выступает приложение с графическим интерфейсом, которое устанавливается на ПЭВМ. Приложение было разработано для сертификации в одной из лабораторий компании EMVCo, по требованиям к этому ПО интерфейс приложения – английский, для сертификации ядра "МИР" в приложение был добавлен необходимый функционал. В качестве примера аппаратной платформы в данном документе будет рассмотрен ридер "BCAM-01", разработанный российской компанией ООО "Социальные системы". Протокол обмена и управления "BCAM-01" - PB3P, разработанный также ООО "Социальные системы".

1.1. Требования к программным и техническим средствам

Для работы с ядром "МИР", где терминальной программой является приложение, установленное на ПЭВМ, и с выбранной аппаратной платформой "BCAM-01" требуется:

- инструментальная ПЭВМ под управлением ОС Windows, версии не ниже 8, с установленной на ПЭВМ программой "L2 Test Environment" (далее TEI), версии не ниже 1.2.0;

- устройство "BCAM-01" с загруженной на него рабочей программой, версии не ниже 2.5.1, с модулем ядра "МИР", версии не ниже 1.0.1; устройство должно быть подключено к ПЭВМ по USB-кабелю;

- банковская карты, выпущенная с приложением МИР, с бесконтактным интерфейсом.

1.2. Начало работы

Для начала работы требуется запустить приложение TEI, открыть вкладку 'Settings', выбрать порт, который назначен для ридера, нажать на форме кнопку 'Open'. Приложение TEI откроет порт, автоматически опросит версии ПО ридера и выведет их в поле 'Versions' (рисунок 1).

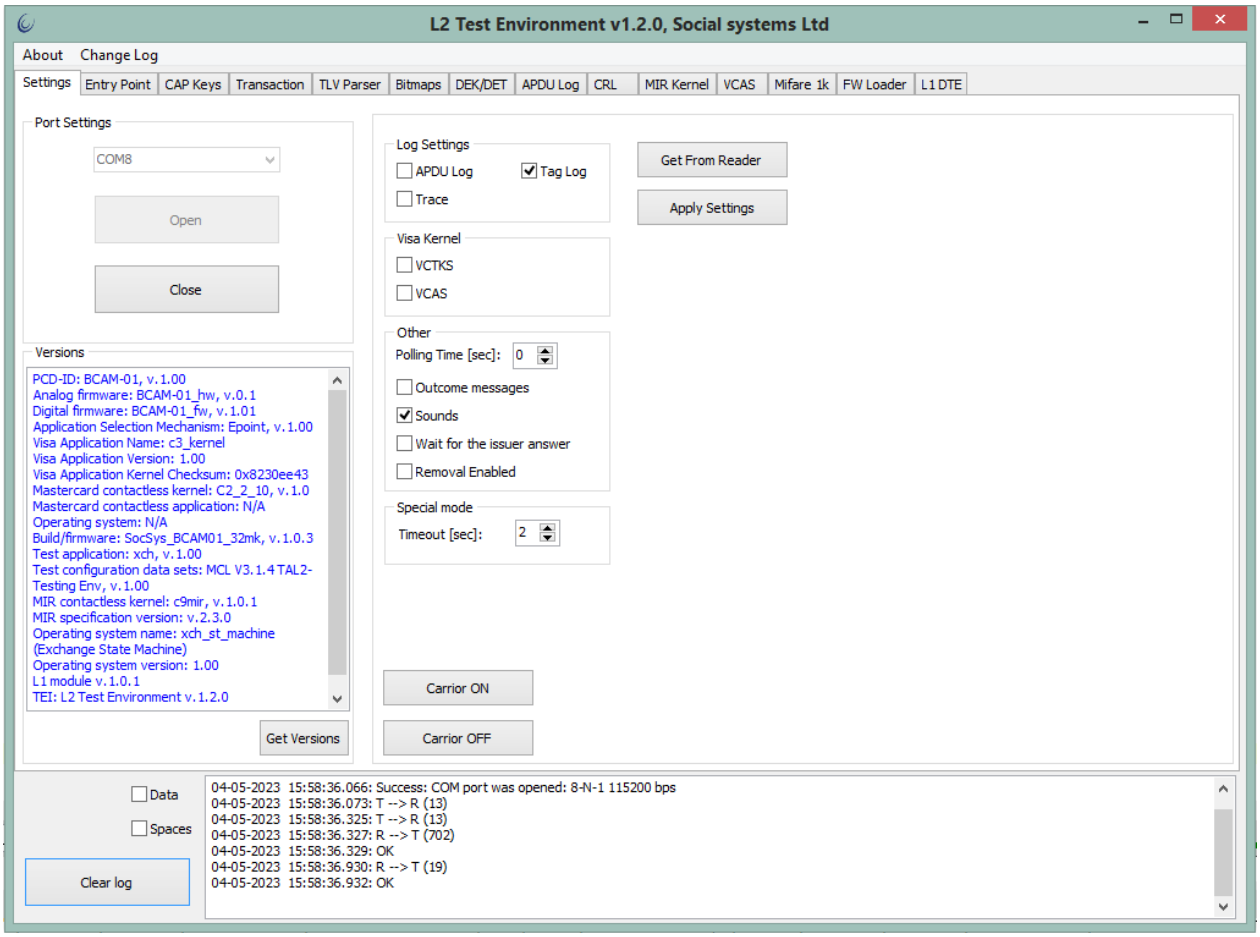

Рисунок 1 - Начало работы, открытие порта.

2. Эксплуатация ядра "МИР"

2.1. Настройки ядра "МИР"

Архитектура программного обеспечения ядра "МИР" позволяет:

- вводить настройки как для отдельных платёжных приложений (AID), так и для группы платёжных приложений;
- вводить настройки для каждого типа поддерживаемых операций.

Поддерживаются следующие настройки ядра:

- обозначение терминала (Terminal Identification);
- настройки терминала относительно режима обработки транзакции (Terminal TPM Capabilities);
- тип терминала (Terminal Type);
- спецификаторы для принятия решений ядром на основании результатов проведения транзакции (TVR) - (TAC Denial, TAC offline, TAC online);
- настраиваемый счётчик попыток восстановления транзакции (Transaction Recovery Limit);
- поддерживаемая версия платёжного приложения карты (Application Version Number);
- список запрашиваемых тегов в режиме прямого обмена с ядром (Data Exchange Tag List);
- сумма транзакции, при превышении которой принимается решение авторизации транзакции в онлайн-режиме (Terminal Floor Limit);
- максимальная сумма транзакции, допустимая при использовании бесконтактного интерфейса (Terminal Contactless Limit (CD-CVM/Non CD-CVM));
- максимальная сумма транзакции, при которой транзакция может проводиться без проверки держателя карты (Terminal No CVM Limit).

Для реализации данного функционала в приложении TEI предусмотрены элементы управления. Для задания настроек ядра "МИР" следует открыть вкладку 'Entry Point'. В левой части окна, в секции 'Processing Configuration', добавить AIP (номер приложения) 'A000000658', нажав на кнопку 'Add'. В правой части, в секции 'EP configuration', добавить запись с настройками (кнопка 'Add'), изменить поле 'Kernel ID', кликнув на поле и выбрав из списка элемент 'MIR', слева от созданной записи нажать на 'Edit...' (рисунок 2). Откроется форма, в которой можно вводить обозначенные в данном пункте настройки (рисунок 3), в конце изменений следует нажать кнопку 'Accept'.

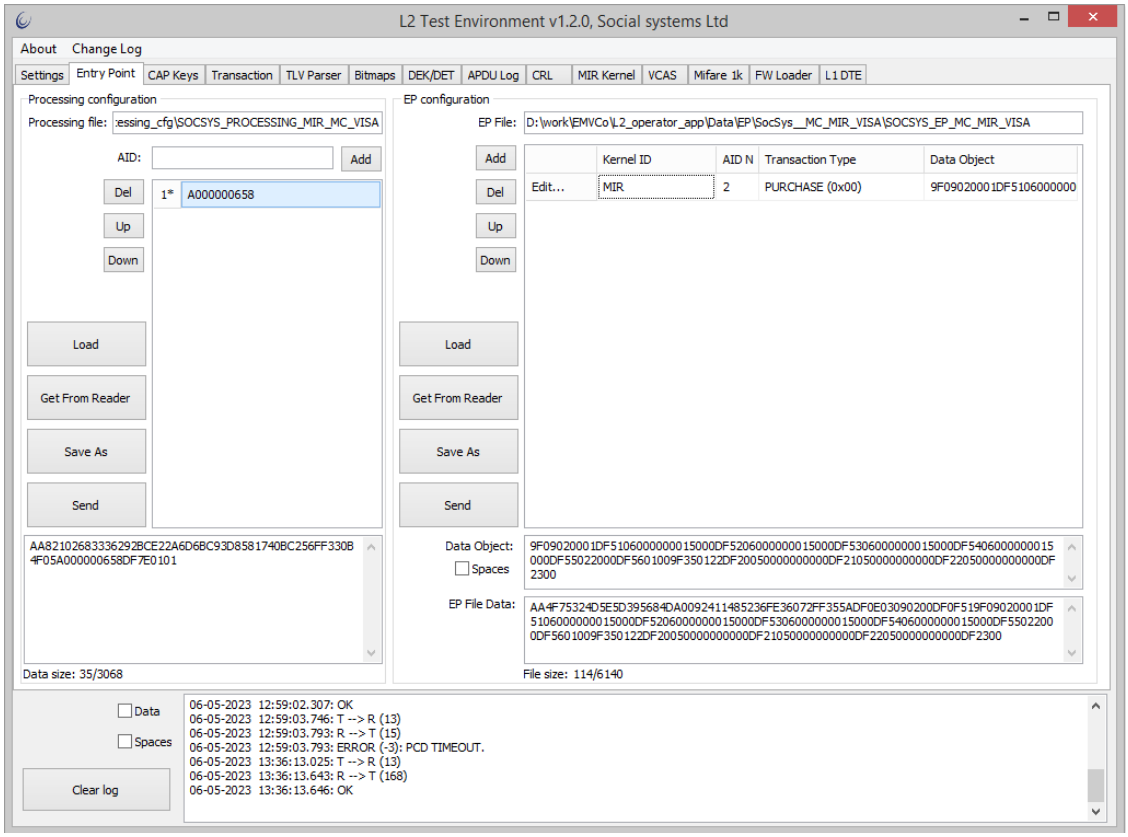

Рисунок 2 - Добавление поддерживаемых AID и настроек для AID.

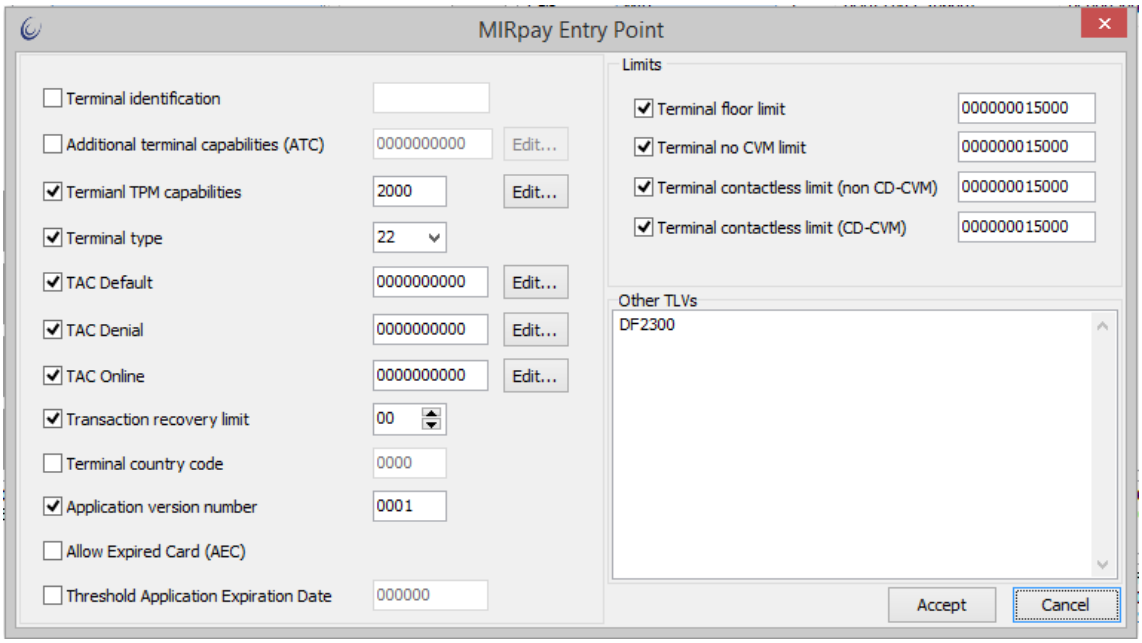

Рисунок 3 – Настройки бесконтактного ядра "МИР"

После внесения изменений настройки следует отправить в ридер, для этого необходимо в секциях 'Processing Configuration' и 'EP configuration' нажать кнопку 'Send'.

2.2. Поддерживаемые операции

Поддерживаются следующие типы операций:
- оплата товара/услуги с использованием карты - Purchase;
- выдача наличных - Cash;
- покупка с выдачей наличных - Purchase with Cashback;
- возврат денежных средств - Refund;
- внесение наличных - Cash Deposit;
- выдача наличных с участием оператора - Manual Cash;
- и другие.

Тип операции задаётся при конфигурировании ядра "МИР" (пункт 2.1 настоящего документа). Для задания поддерживаемой операции на вкладке 'Entry Point', в секции 'EP configuration' необходимо кликнуть на сформированной записи в поле 'Transaction Type' и выбрать из списка необходимую операцию (Рисунок 2). Для каждой тройки 'Kernel ID - AID N - Transaction Type' требуется своя конфигурационная запись.

Ядром «МИР» поддерживается административная операция отмены транзакции. Для исполнения этой команды ядром «МИР» необходима предварительная команда начала транзакции. Чтобы начать транзакцию, необходимо на вкладке 'Settings' полю 'Polling Time' присвоить значение 20 [секунд], нажать кнопку на форме 'Apply Settings'. Далее требуется перейти на вкладку 'Transaction' и нажать кнопку 'Start transaction', приложение пошлёт команду ридеру и будет в течение 20 секунд ожидать результата транзакции. Отменить транзакцию можно, нажав на кнопку 'Cancel' на той же вкладке 'Transaction', ридер ответит на команду результатом '-130' ("Cancelled by user") (рисунок 4).

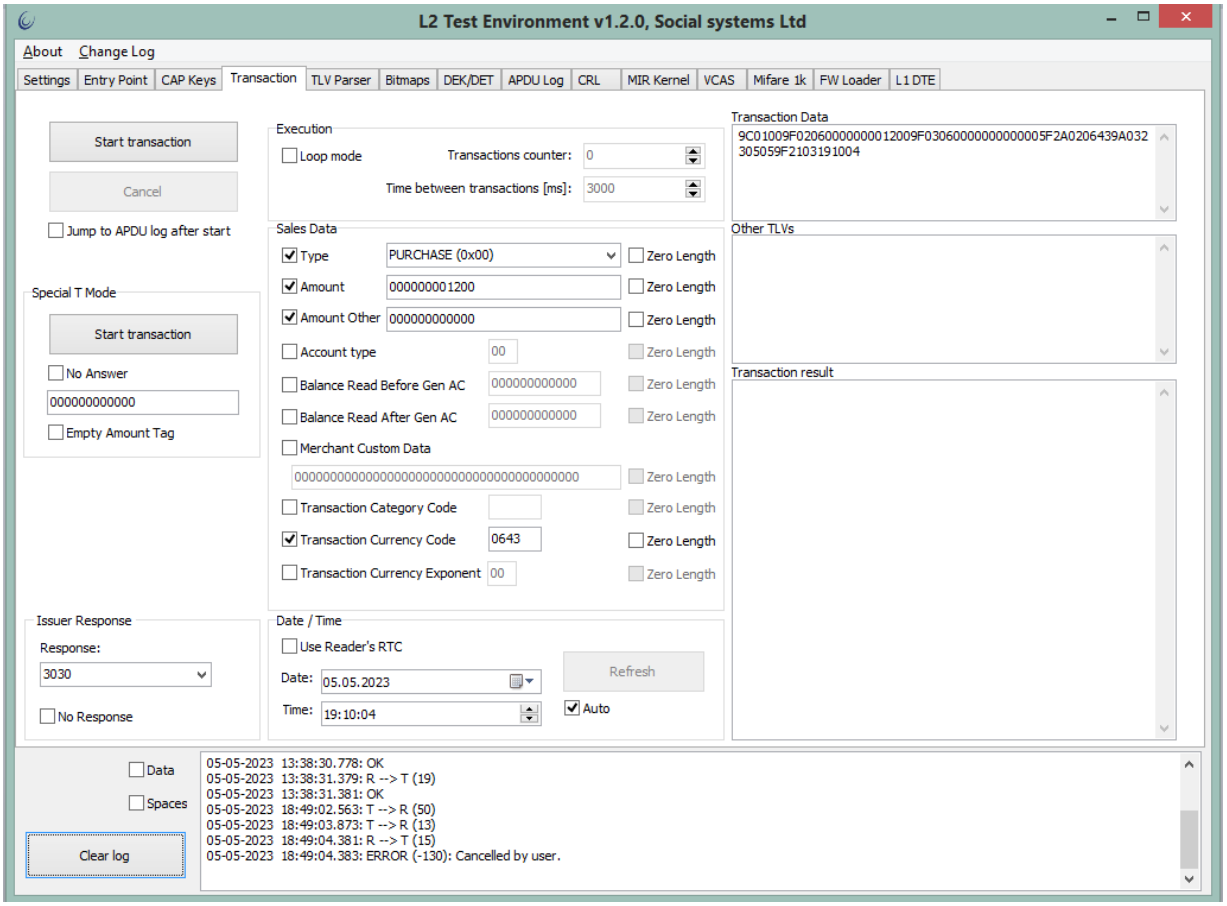

Рисунок 4 - Результат команды отмены транзакции. В нижней части формы, в консоли.

2.3. Поддержка работы со списком открытых ключей аутентификации (CAPK)

Ядро "МИР" поддерживает работу со списком открытых ключей аутентификации: чтение и поиск ключа по индексу.

Для составления списка в приложении TEI предусмотрены элементы управления на вкладке 'CAPK'. Перед началом работы с ядром "МИР" необходимо передать ридеру список CAPK, для этого следует перейти на указанную вкладку в приложении TEI нажать кнопку 'Add' и заполнить поля: RID, Index, Modulus, Exponent. При необходимости повторить по количеству ключей. Сформированный таким образом список CAPK требуется передать ридеру, это можно сделать, нажав кнопку 'Send' на вкладке 'CAPK' (рисунок 5).

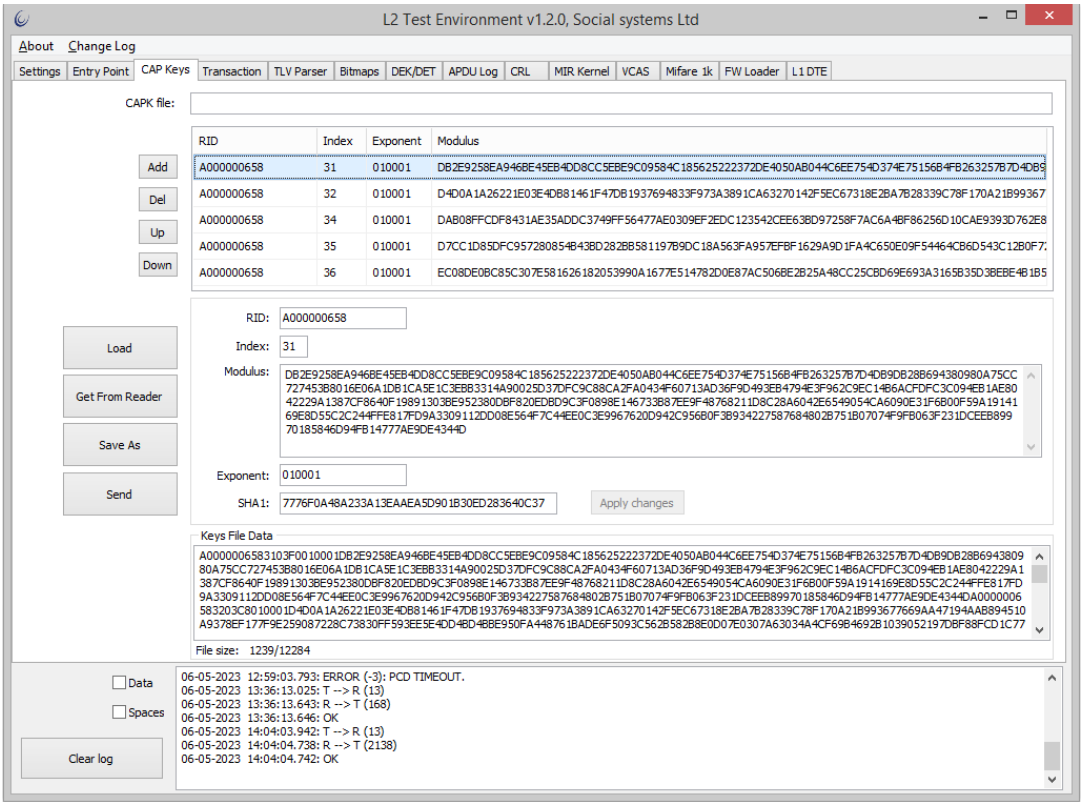

Рисунок 5 - Формирование списка CAPK

2.4. Поддержка сообщений в процессе транзакции (Outcome)

Ядро "МИР" в полном объёме поддерживает выдачу стандартизованных сообщений Outcome.

В процессе транзакции от ридера будут приходить формализованные сообщения в виде посылок PB3P от ридера, их интерпретация - ответственность терминальной программы - в данном случае TEI. В данной реализации в конце транзакции приходит тег, содержащий структуру данных, в которой упакованы необходимые поля для их последующей обработки в терминальной программе (рисунок 6).

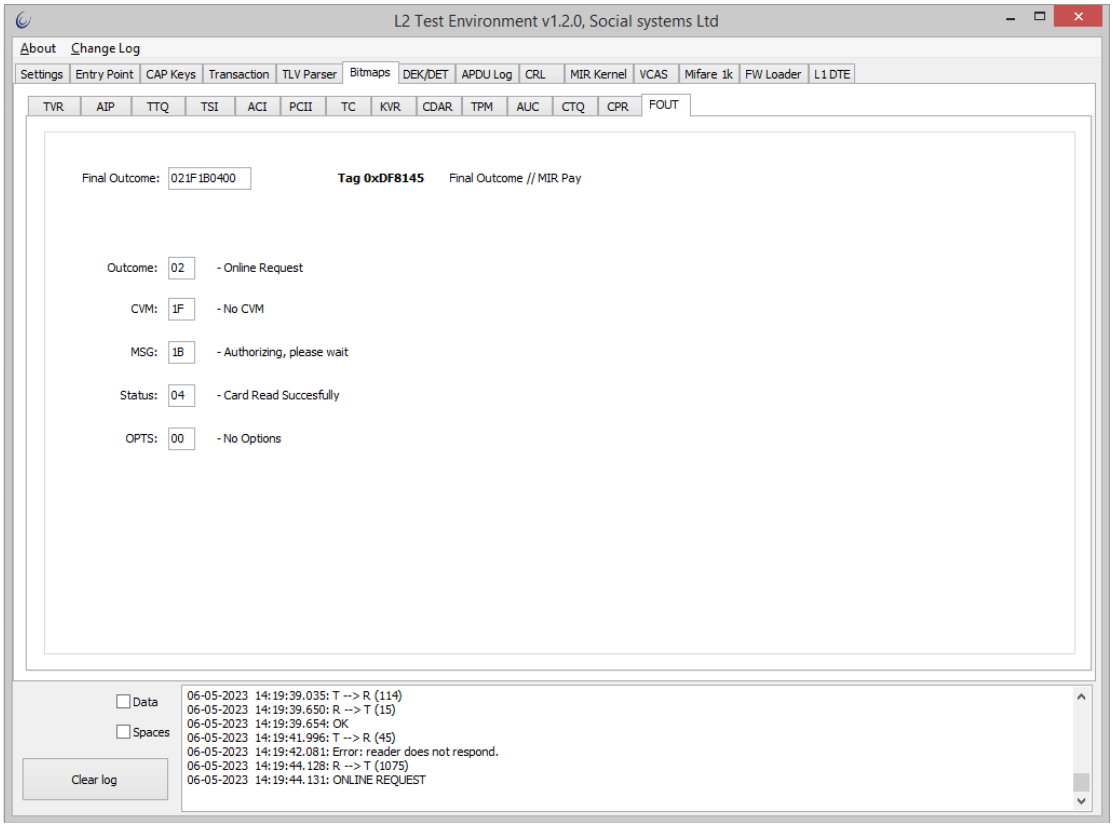

Рисунок 6 – Интерпретация тега Final Outcome, полученного с данными транзакции

2.5. Поддержка протокола прямого обмена данными с ядром во время транзакции (Data Exchange)

Ядро "МИР" в полном объёме поддерживает протокол прямого обмена данными с ядром согласно документу "Спецификация ядра бесконтактного ридера ПС 'МИР'". Для поддержки протокола архитектурой программного обеспечения предусмотрена передача необходимой информации ядру вместе с настройками.

Прямой обмен с ядром выполняется в соответствии со спецификацией бесконтактного ядра «МИР». Для обмена в спецификации предусмотрен тег ‘Data Exchange Tag List’, числовое значение которого разработчик назначает самостоятельно, для данной реализации ядра «МИР» - это тег ‘DF2300’. Его значение задаётся в конфигурации ядра в поле ‘Other TLVs’ (в реализации приложения TEI) (рисунок 3).

2.6. Поддержка режимов работы ядра

В зависимости от типа терминала ядро "МИР" поддерживает работу в следующих режимах:

- только онлайн (online-only);
- только оффлайн (offline-only);

- оффлайн с возможностью онлайн (offline with online capability).

Режим работы регулируется настройками ядра "МИР", в частности 'Terminal Type'. Значение 'Terminal Type' выставляется на форме настроек ядра «МИР» - форма 'MIRpay Entry Point' (рисунок 3).

2.7. Восстановление транзакции

Ядро "МИР" поддерживает механизм восстановления прерванной транзакции. Количество попыток восстановления задаётся в настройках ядра (Transaction Recovery Limit), на форме настроек ядра «МИР» - форма 'MIRpay Entry Point' (рисунок 3).

2.8. Режим работы с инфраструктурой чипа карты (EMV Mode)

Ядро «МИР» в полном объёме поддерживает работу в режиме EMV с выдачей минимального требуемого объёма данных транзакции, кроме того, ядро предоставляет возможность выдачи всего объёма данных (всех тегов, полученных во время транзакции).

Ридер в конце транзакции присылает результат и данные транзакции. В приложении TEI теги транзакции помещаются в поле 'Transaction result' на вкладке 'Transaction' (рисунок 7). В нижней части окна приложения - в консоли - выводится результат: ERROR в случае ошибки, Online Request в случае, когда необходим ответ эмитента, Approved в случае, когда транзакция одобрена в offline, и Decline в случае отклонения транзакции. Данные транзакции представляют собой набор тегов, записанных в формате BER-TLV, просмотреть которые можно дважды щёлкнув мышкой на поле 'Transaction result', в этом случае приложение переключится на вкладку 'TLV Parser' (рисунок 8).

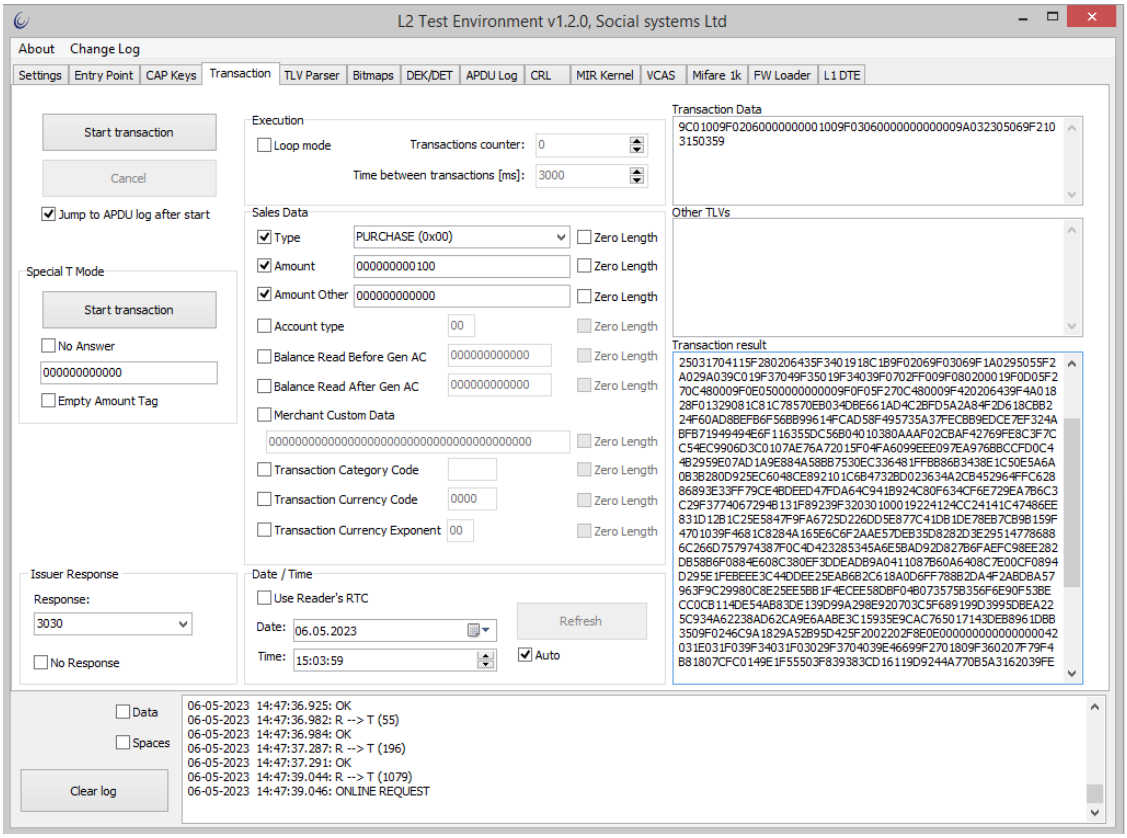

Рисунок 7 - Результат проведения транзакции (Online Request)

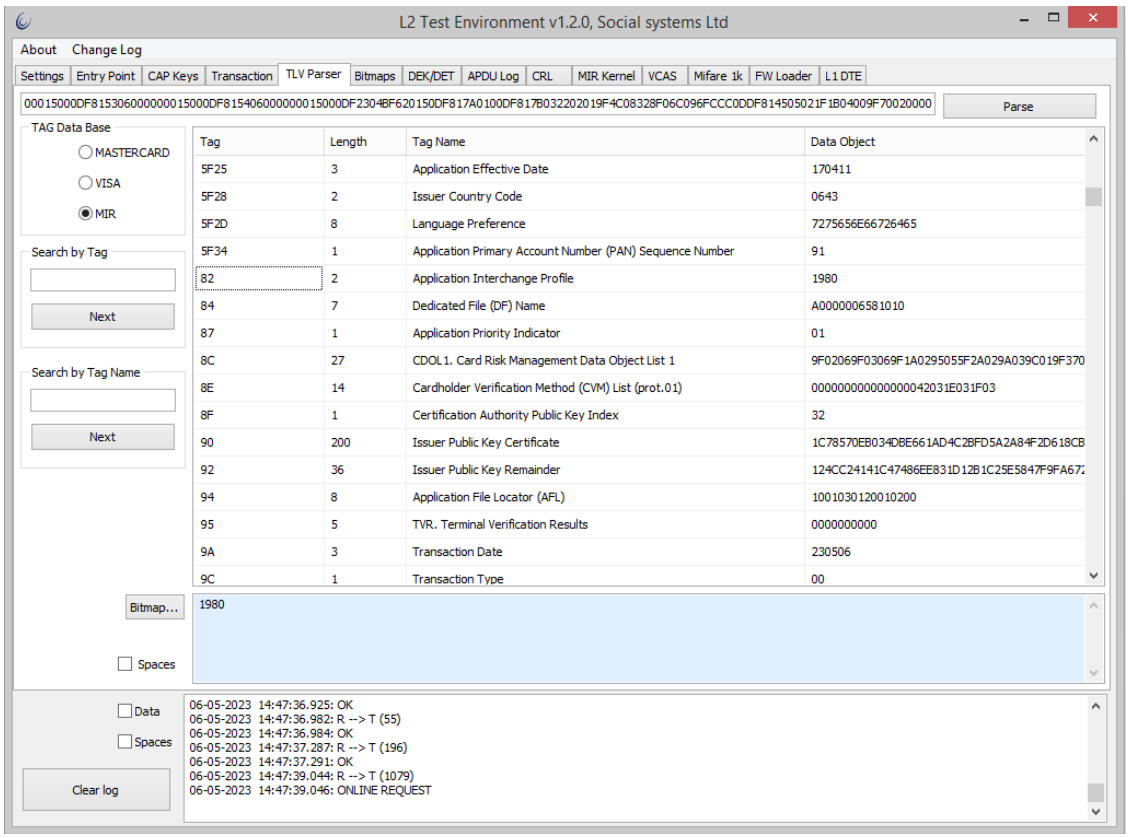

Рисунок 8 - Расшифровка тегов транзакции.

2.9. Аутентификация платёжного приложения

Ядро "МИР" поддерживает единственный метод аутентификации платёжного приложения: CDA - Combined Data Authentication - комбинированная аутентификация. По требованиям ПС "МИР" другие методы, такие как SDA и DDA, не поддерживаются.

Для аутентификации необходим лист CAPK, работа с которым рассмотрена в пункте 2.3 настоящего документа.

2.10. Транзакционные потоки

Ядро "МИР" в полном объёме поддерживает работу по протоколу '01' и по протоколу '02' в соответствии со спецификацией.

Принципиальное отличие протокола ‘02’ от ‘01’ в том, что карта отдаёт все необходимые данные для транзакции на стадии выбора приложения – в ответ на команду ‘SELECT’, а также использует команду ‘PERFORM TRANSACTION’, которая не используется в протоколе ‘01’. Протокол ‘02’ чаще используется на мобильных устройствах.

Увидеть различия между протоколами в приложении TEI можно, отметив поле ‘APDU Log’ на вкладке ‘Settings’, применив изменения настроек (кнопка ‘Apply Settings’) (рисунок 1) и проведя две транзакции: одну с мобильным устройством (например, с приложением MIR Pay) и одну с помощью пластиковой банковской карты с бесконтактным интерфейсом. В приложении TEI транзакцию можно провести, нажав на кнопку ‘Start Transaction’ на вкладке ‘Transaction’, а посмотреть лог обмена ридера и карты можно на вкладке ‘APDU Log’.

Обмен по протоколу ‘01’:

```
CAPDU (PPSE):
00A404000E325041592E5359532E444446303100


RAPDU:
6F23840E325041592E5359532E4444463031A511BF0C0E610C4F07A000000658101087010190000


CAPDU (SELECT):
00A4040007A000000658101000


RAPDU:
6F388407A0000006581010A52D8701019F380F9F7A015F2A029F02069F35019F40055F2D087275656E667
26465BF0C059F4D02180A50034D49529000


CAPDU (GPO - GET PROCESSING OPTIONS):
80A8000011830F000643000000001100220000000000000
```

RAPDU:
770E8202198094081001030120010200900 0

CAPDU (READ RECORD):
00B2011400

RAPDU:
7081875710220070013199000D2505201147036795A0822007001319900005F24032505315F250317041
15F280206435F3401918C1B9F02069F03069F1A0295055F2A029A039C019F37049F35019F34038D0C9108
8A0295059F37049F4C089F0702FF009F080200019F0D05F270C480009F0E0500000000009F0F05F270C48
0009F420206439F4A01829000

CAPDU (READ RECORD):
00B2021400

RAPDU:
7081CE8F01329081C81C78570EB034DBE661AD4C2BFD5A2A84F2D618CBB224F60AD8BEFB6F56BB99614FC
AD58F495735A37FECBB9EDCE7EF324ABFB71949494E6F116355DC56B04010380AAAF02CBAF42769FE8C3F
7CC54EC9906D3C0107AE76A72015F04FA6099EEE097EA976BBCCFD0C44B2959E07AD1A9E884A58BB7530E
C336481FFBB86B3438E1C50E5A6A0B3B280D925EC6048CE892101C6B4732BD023634A2CB452964FFC6288
6893E33FF79CE4BDEED47FDA64C941B924C80F634CF6E729EA7B6C3C29F3774067294B131F89239000

CAPDU (READ RECORD):
00B2031400

RAPDU:
70309F32030100019224124CC24141C47486EE831D12B1C25E5847F9FA6725D226DD5E877C41DB1DE78EB
7CB9B159F4701039000

CAPDU (READ RECORD):
00B2012400

RAPDU:
7081D19F4681C8284A165E6C6F2AAE57DEB35D8282D3E295147786886C266D757974387F0C4D423285345
A6E5BAD92D827B6FAEFC98EE282DB58B6F0884E608C380EF3DDEADB9A0411087B60A6408C7E00CF0894D2
95E1FEBEEE3C44DDEE25EAB6B2C618A0D6FF788B2DA4F2ABDBA57963F9C29980C8E25EE5BB1F4ECEE58DB
F04B073575B356F6E90F53BECC0CB114DE54AB83DE139D99A298E920703C5F689199D3995DBEA225C934A
62238AD62CA9E6AABE3C15935E9CAC765017143DEB8961DBB3509F0246C9A1829A52B95D425F2002202F9
000

CAPDU (READ RECORD):
00B2022400

RAPDU:
70108E0E0000000000000000042031E031F039000

CAPDU (GAC - GENERATE AC):

```
80AE500021000000001100000000000000064300000000000064323050600E7C0C6E9221F030200


RAPDU:
7781B09F2701809F360207FC9F4B8180B31B862318615F4735512735DA41605AB04E5D06763A2FB0C60CB
AF003396413C535D2A0849EFCE7436C6C3BC02CC5249830781FC309083B43D1D206A2B051B39C4DF619D8
24D6C1A4CA79FE24C3EB90D2F8962B7D6421A3092187A21CE8AD181CCE5F792597BA67088499BE7E20C60
BD74D58E85218847E3E7679D4A5B5ACAE9F10200FA501A8302020003DD98C7589A676E010040000000000
000000000000000009000
```

Обмен по протоколу ‘02’:

```
CAPDU (PPSE):
00A404000E325041592E5359532E444446303100


RAPDU:
6F29840E325041592E5359532E4444463031A517BF0C1461124F07A0000006581010870101 9F2A038106439000


CAPDU (SELECT):
00A4040007A000000658101000


RAPDU:
6F81A98407A0000006581010A5819D8701015F2D047275656E50074D495220504159BF61415A0A2200700
217955582000F5F24032711309F0702FFC09F420206435F280206439F241D4E303338303030303030303030
303030303030303030303030304C413030BF621F5F340100570E2200700217955582000D2711201F9F080
200015F2503221124DF70050101020340DF6F19DF71029F02069F03069F1A025F2A029A039C019F37049F
35019000


CAPDU (PERFORM TRANSACTION):
80A600001B2002000000001100000000000000064306432305060 0FF01999D2200


RAPDU:
773C9F710201809F2608A413B64D118B5A519F2701809F360201579F10200FB6012000000001000000000
00000FF087B000000000000000000000000103269000
```

2.11. Работа с отозванными сертификатами (CRL)

Ядро "МИР" поддерживает работу со списком отозванных сертификатов.

Список отозванных сертификатов загружается в ридер наряду с настройками ядра. Создать и загрузить в ридер список отозванных сертификатов (CRL) можно в приложении TEI на вкладке 'CRL' (рисунок 9). Отправить список в ридер можно, нажав кнопку 'Send'.

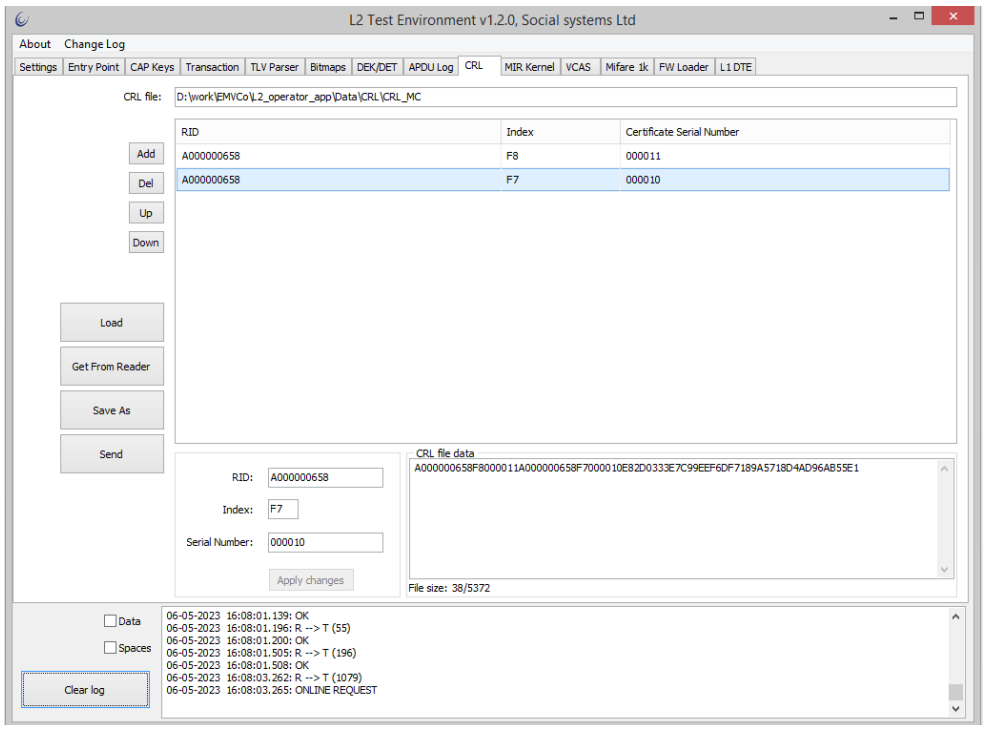

Рисунок 9 - Формирование и отправка ридеру списка отозванных сертификатов.